



Timothy C. Parlatore, Esq.
Founder & Managing Partner

October 29, 2018

AUSA Paul Murphy
United States Attorney's Office, District of New Jersey
970 Broad Street, 7th Floor
Newark, NJ 07102

RE: United States v. Paul Parmar, Criminal No. 18-mj-8040

Dear AUSA Murphy:

As you are aware, I represent Paul Parmar, along with Jeffrey Hoffman of Windels Marx. As Mr. Hoffman is currently preparing for a trial, he asked me to reach out to you directly on this emergent issue. As we have discussed in the past, we believe that there has been a concerted effort by Chinh Chu to threaten and intimidate Mr. Parmar into pleading guilty in this case. The purpose of this letter is to provide you with an update on these activities and to urgently request your assistance, as a federal law enforcement officer, to address these ongoing criminal activities.

Bottom line up front – Chinh Chu has admitted that he hired the team of people who have been following and intimidating Mr. Parmar's family.¹ Moreover, Chinh Chu has admitted to putting Mr. Parmar's home under constant surveillance at the exact same time that someone illegally hacked into his home server and downloaded a massive amount of data.

Through a DMV license plate search, we identified Victor Cardona and James Stepien as two of the individuals who were outside of Mr. Parmar's home. Victor Cardona is an active member of the NYPD and James Stepien is a convicted felon, currently on probation. Mr. Cardona and Mr. Stepien were hired by a private investigator named Warren Ernst.² Warren Ernst was hired by Tony Schiena of Multi Operational Security Agency Intelligence Company ("MOSAIC").

MOSAIC is a private military contracting company, run by Mr. Schiena, who bills himself as the "world's most highly trained covert operative."³ However, in addition to fighting ISIS in Kurdistan and chasing human traffickers, MOSAIC provides services in "asset recovery" and "cybersecurity." The advertised cybersecurity services include testing systems:

¹ A copy of Chinh Chu's declaration is annexed hereto at Exhibit "A."

² Mr. Ernst's actions in providing private investigative services in New Jersey without a New Jersey license, the employment of an unlicensed off-duty police officer and the employment of a convicted felon present a whole host of issues in violation of various New Jersey state statutes.

³ Mr. Schiena's Wikipedia biography is annexed hereto at Exhibit "B."

utilizing a series of techniques including attacking software and computer systems from the start by scanning ports, and examining known defects and patch installations. Attack types include social engineering, open source research, and deception to attempt a cyber attack in order to bypass and breach your perimeter and physical security, within an agreed set of boundaries.⁴

This advertised service is exactly what Mr. Parmar fears Mr. Chu did to his home system.

MOSAIC was hired directly by Chu or CC Capital to perform cybersecurity services, as well as to surveil Mr. Parmar's home and family. MOSAIC subcontracted surveillance services to Ernst and, potentially, others. This is not speculation, as the involved parties have all admitted that this was the arrangement. While they may deny nefarious purposes or the full scope of their activities, they are unable to deny their involvement.

Particularly relevant to the hacking of Mr. Parmar's data, Mr. Chu admits that his team surveilled Mr. Parmar's house "from September 8-11." Photos show that Cardona parked his car directly across from Parmar's front gate during that time. It can be no coincidence that it was during this exact time period that logs show multiple devices accessing Mr. Parmar's network through the front gate access point and downloading massive amounts of data. Below are photos of the logs for the front gate access point:

The image displays four screenshots of a network monitoring application, likely Wireshark or a similar tool, showing the 'PROPERTIES' window for different Android devices. Each window has tabs for 'Details', 'History', and 'Configuration'. The 'Overview' and 'Statistics' sections are visible in each window.

Device 1: android-1e6f7a844e226056

- MAC Address: 08:d4:6aa4:80:ec
- Hostname: android-1e6f7a844e226056
- Device Type: [Icon]
- IP Address: 192.168.2.135
- Uptime: 2h 11m 57s
- Connected AP: GATE
- ESSID: Parmar

Device 2: android-6e159763e6951e55

DATE/TIME	DURATION	DOWN	UP
09/11/2018 7:44 pm	15m 57s	8.09 KB	16.1 KB
09/11/2018 3:15 pm	2h 31m 32s	816 KB	349 KB
09/10/2018 8:11 pm	16h 55m 41s	2.02 MB	1.54 MB
09/10/2018 7:35 pm	41m 18s	277 KB	170 KB
09/09/2018 6:18 pm	23h 13m 59s	436 MB	19.9 MB

Device 3: android-5b52490ec105082c

- Activity: 52,034,286 / 48 GB
- Down Pkts/Bytes: 52,034,286 / 48 GB
- Up Pkts/Bytes: 48,304,197 / 25.5 GB

Device 4: android-f821fed052dc1fc

- Activity: 0 bps
- Down Pkts/Bytes: 22,491,392 / 25.3 GB
- Up Pkts/Bytes: 22,837,318 / 16.1 GB

Device 5: android-6e159763e6951e55

- Activity: 7,499,608 / 7.66 GB
- Down Pkts/Bytes: 7,499,608 / 7.66 GB
- Up Pkts/Bytes: 6,217,330 / 1.78 GB

Device 6: android-5b52490ec105082c

DATE/TIME	DURATION	DOWN	UP
09/08/2018 7:33 pm	3d 13h 15m 39s	4.04 MB	706 KB
09/07/2018 6:27 pm	10m 40s	6.01 KB	12.8 KB
09/07/2018 6:26 pm	20h 53m 48s	26.5 MB	3.6 MB
09/07/2018 5:34 pm	13m 4s	1.38 MB	388 KB
09/07/2018 12:06 pm	43m 25s	57.3 MB	3.01 MB

⁴ A printout of the MOSAIC website is annexed hereto at Exhibit "C."

There can be only two possible explanations for the undisputable fact that someone accessed and downloaded all of this data at the exact same time that Mr. Chu's team was surveilling the gate: either Chu's team is behind the hack or they surveilled whoever did. The hacker accessed the system through the wireless access point, so they would have had to be within close physical proximity to the gate.

As part of our investigation, I have been in contact with the attorney for Mr. Ernst, Mr. Cardona and Mr. Stepien and we had been working to resolve his clients' involvement. Unfortunately, these efforts fell apart last night, as I received written communication indicating that Mr. Ernst may have been the victim of an intimidation effort by Mr. Chu, Mr. Schiena, or both:

Please note that on Friday, 26 October 2018, morning, I was contacted by Warren, who advised that his automobile was entered that night/morning and property stolen. He further advised that the person/persons who entered his car then accessed personal items and then remotely started his car in the early morning on 26 October 2018. The New York Police Department was dispatched and are presently investigating. Warren has removed his family from his family residence due to the fear that the same persons who are the subject of your order to show cause or a party to the litigation may have been sending him a "message" and may in fact attempt to cause harm to him or his family.

Clearly, the witness intimidation efforts in this case have gone far past only targeting my client and Mr. Ernst has no motive to lie about what happened to him. What is particularly disturbing is that Mr. Ernst is a retired police officer, licensed to carry a firearm. It appears that Mr. Chu is unafraid to threaten a trained and armed man, whereas my client is an unarmed sitting duck on home confinement.

While we certainly appreciate the adversarial relationship that ordinarily exists between your office and criminal defendants, the circumstances of this case have exceeded all normal bounds. For the sake of my client and public safety, we are asking that you, as a federal law enforcement officer, set aside these differences so that we can work together to address this serious safety concern. My cell phone number is 732-904-6391.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Timothy C. Parlatore', with a stylized, flowing script.

Timothy C. Parlatore, Esq.

Exhibit A

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

-----X

ALPHA CEPHEUS, LLC
FIRST UNITED HEALTH, LLC,
CONSTELLATION HEALTH, LLC
NAYA CONSTELLATION HEALTH, LLC and
CONSTELLATION HEALTH INVESTMENT,
LLC,

Plaintiffs,

No.: 18-cv-14322 (MCA)

v.

CHINH CHU,
TRUC TO,
DOUGLAS NEWTON,
JAMES STEPIEN,
VICTOR CARDONA, and
JOHN DOE 1-10,

Defendants.

-----X

**DECLARATION OF CHINH CHU IN SUPPORT OF DEFENDANTS CHINH CHU AND
DOUGLAS NEWTON'S OPPOSITION TO PLAINTIFFS' MOTION FOR A
PRELIMINARY INJUNCTION**

I, CHINH CHU, hereby affirm under penalty of perjury in accordance with the laws of the United States, that the following is true and correct:

1. I am the founder and Senior Managing Director of CC Capital Management LLC ("CC Capital"), a private investment firm based in New York City. Prior to founding CC Capital, I worked in private equity for twenty-five years at Blackstone Group L.P., where I ultimately served as co-chairman of the firm's Private Equity Investment Committee and on the firm's Executive Committee. I submit this affidavit in support of Defendants' opposition to the October 19, 2018 Order to Show Cause (the "OSC") in the above-referenced matter. The OSC accuses me of extraordinary wrongdoing. As set forth below, these accusations are completely false.

The CHT Transaction

2. Beginning in and around early 2016, CC Capital identified Constellation Healthcare Technologies, LLC (“CHT”) as a potential acquisition. At that time, I first became acquainted with Paul Parmar in his capacity as Chief Executive Officer of CHT. CHT was a publicly traded company prior to 2016. CC Capital and the Board of Directors of CHT negotiated a “Go-Private” transaction in which the shares of CHT common stock would be cancelled and converted into the right to receive cash and a promissory note, and the publicly traded company would be converted into a private entity.
3. On November 24, 2016, CC Capital consummated this deal (the “Go-Private Transaction”), and the transaction closed on January 30, 2017. At closing, CC Capital controlled 50.7% of the economic and 55% of the voting interests in CHT. As part of the financing for the transaction, CC Capital contributed approximately \$82 million in equity, most of which came from me personally. A consortium of financial institutions including Bank of America provided another approximately \$130 million in debt. I am aware of legal filings that say that Mr. Parmar and entities he controlled stood to receive approximately \$100 million in the transaction.

Parmar’s Fraud

4. Subsequent to closing of the CHT transaction, facts emerged indicating that Mr. Parmar had engaged in a complex and brazen fraud to induce CC Capital to acquire a controlling interest in CHT. Mr. Parmar resigned from CHT, and an outside forensic investigation team was brought in to determine the extent of the fraudulent activity. Declaration of Timothy J. Dragelin (“Dragelin Decl.”), ¶ 88 (attached as Exhibit 1). As this fraud unraveled, on March 16, 2018, certain affiliates of CHT (the “CHT Debtors”) filed voluntary petitions for relief under Chapter 11 of the bankruptcy code in the United States Bankruptcy Court for the Eastern District of New York. The debtors in the bankruptcy proceeding attributed CHT’s bankruptcy to Mr. Parmar’s fraudulent conduct. *Id.* ¶¶ 9, 88-91, 111.
5. Prior to bankruptcy, CHT retained a Chief Restructuring Officer (“CRO”) and brought in an independent director to ensure proper corporate governance and absence of conflicts in connection with the decision about whether to file for bankruptcy and how the CHT debtors would proceed after filing bankruptcy. Neither I, nor anyone affiliated with CC Capital, were decision makers regarding whether CHT or any of its affiliates would file for bankruptcy or any litigation or claims that the CHT debtors are pursuing against third-parties including Parmar.
6. Since the March 2018 bankruptcy filing, the CHT Debtors have continued to be managed by the CRO with the oversight of an independent director in proceedings administered by United States Bankruptcy Judge Alan Trust. There is an active creditors’ committee in these bankruptcy proceedings. Neither I nor anyone else affiliated with CC Capital plays

any role on the creditor's committee which represents the interests of the creditors of the CHT debtors, including the consortium of lenders in the Go-Private Transaction.

The Criminal Charges and Other Litigation against Parmar

7. On May 16, 2018, the United States Attorney's Office for the District of New Jersey brought securities fraud charges against Mr. Parmar in connection with the Go-Private Transaction. Attached as Exhibit 2 is the Criminal Complaint filed against Mr. Parmar and several co-conspirators. CC Capital is the "Private Investment Firm" referred to in this Complaint as the victim of Mr. Parmar's alleged securities fraud.
8. The Securities and Exchange Commission ("SEC") similarly brought a civil action against Mr. Parmar on May 16, 2018, charging Parmar with securities fraud in the Go-Private transaction. Attached as Exhibit 3 is a Complaint filed by the SEC against Paul Parmar on May 16, 2018. CC Capital is "Investor-1" referred to in this Complaint as the victim of Mr. Parmar's alleged securities fraud.
9. In the bankruptcy proceeding, the CHT Debtors have also sued Mr. Parmar and certain of his affiliates for fraud and theft in connection in the Go-Private transaction. Attached as Exhibit 4 is the Complaint in the Adversary Proceeding against Mr Parmar and others in the bankruptcy.
10. I understand that Mr. Parmar was arrested on May 16, 2018 based on the Criminal Complaint, and then was then incarcerated for several months until he was released after posting bail in July 2018. Attached as Exhibit 5 is the Amended Order Setting Conditions of Release in Mr. Parmar's criminal case in the United States District Court for the District of New Jersey. This Order requires Mr. Parmar (i) to post bail in the amount of \$3,462,911.00 as a condition of his release and (ii) to remain at his residence in New Jersey at all times, except to meet with counsel and other limited exceptions.

Mr. Parmar's False Accusations of Harassment and Intimidation

11. Mr. Parmar's conduct has exposed me and my firm to significant financial and reputational harm. On top of that, earlier this year I became concerned that Mr. Parmar posed a potential threat to me and my children, and that he might be engaged in ongoing wrongful conduct targeting me and my firm.
12. I consulted with a security consulting firm to get recommendations about how to address these issues. Following their advice, I engaged the firm to conduct a cybersecurity analysis and determine whether my computer or phone might be bugged or otherwise monitored. The firm also conducted background checks regarding Mr. Parmar. I also used the firm to arrange for an off-duty New York City Police Officer to provide protection for my children. These protection services are ongoing.

13. In July, Mr. Parmar was released from jail. During the summer, he and entities associated with him began to make legal filings with extraordinary, false accusations that I was the mastermind behind a fraud involving CHT and that Mr. Parmar was the victim, rather than the culpable party. Given these developments, I became concerned that Mr. Parmar was becoming increasingly desperate and might take rash action. In light of such concerns, the security firm advising me recommended that I consider surveillance to try to assess the potential threat to me or my family from Mr. Parmar's activities. In discussing this recommendation, I told the security firm that any such activities would have to be lawful. They assured me that any activities undertaken by them, or at their direction, would be lawful.
14. Because Mr. Parmar's temporary release conditions confined him to his residence with limited exceptions, the security firm believed that he might rely on others to coordinate activities on his behalf. Thus, the security firm recommended that it arrange for surveillance of Mr. Parmar's residence and the activities of individuals who might come and go from his residence. I was told that this surveillance would be undertaken under proper lawful protocols, including notification to, and coordination with, the local police department.
15. I have been told that this surveillance occurred for four days, from September 8-11. When the surveillance concluded, I was provided a high-level summary. I did not authorize, and I am not aware of, any further surveillance activities of Mr. Parmar, people affiliated with Mr. Parmar, or any member of Mr. Parmar's family beyond these four days in September.
16. To be clear, I have never authorized or instructed any security firm or other individual to engage in activities in regards to Mr. Parmar beyond the above-described security services, nor am I aware of any conduct that occurred beyond these services.
17. To that end, I can unambiguously attest that:
 - a. I have never authorized or instructed anyone to threaten or harass Mr. Parmar or his family in connection with this litigation, his criminal proceeding, or otherwise. To my knowledge, no such threats or harassment have ever occurred, and the security firm told me that nothing that they did in the course of performing security services involved threatening or harassing Mr. Parmar or his family.
 - b. I have never authorized, instructed, or known about any "hacking" or other interception of Mr. Parmar's wireless network, or any other of Mr. Parmar's telephonic or digital communications. To my knowledge, no such "hacking" occurred, and the security firm has expressly told me that nothing that they did in the course of performing security services involved "hacking" or otherwise

monitoring or misappropriating the electronic communications of Mr. Parmar or his family or anyone else.

- c. Contrary to Mr. Parmar's claim, I have never suggested to Mr. Parmar that I worked with either the "Chinese Mafia" or "ex-NSA agents" who could kidnap, interrogate, or otherwise threaten Parmar or hack into his network, laptop or phone. Nor have I personally threatened the safety or interests of Mr. Parmar or his family in any other way.
18. To be absolutely clear, I have reviewed Mr. Parmar's October 19, 2018 affidavit and his description of an event that he says occurred on October 10, 2018 in the train station parking lot in Hazlet, New Jersey. I have no knowledge of this incident and, again, I specifically and unequivocally deny that either I or anyone acting at my direction threatened Mr. Parmar or anyone in his family on that day (or ever).
19. Finally, I want to be absolutely transparent about two issues relating to the aforementioned surveillance, including to clear up any misimpressions.
20. First, the Complaint in this action names as defendants two individuals, James Stepien and Victor Cardona, who I understand were retained by a subcontracted security firm to conduct the four days of surveillance referred to above. The Complaint calls these individuals "thugs" and says that Mr. Stepien is a convicted felon. Complaint ¶ 22.
21. Until I saw the Complaint in this action, I had never heard of, and had no knowledge of, either Mr. Stepien or Mr. Cardona. More generally, I had no contact with or knowledge of the individuals that were engaged to undertake the surveillance on September 8-11, 2018.
22. After receiving the Complaint, I contacted the security firm to investigate the issues it raised regarding Mr. Stepien's criminal record.
23. I have since learned that Mr. Cardona is an active member of the New York Police Department and is also the Director of Operations for the security firm engaged as a subcontractor to undertake the surveillance services in September 2018. Mr. Cardona apparently hired Mr. Stepien on the recommendation of officers in the local police department in the town where Mr. Parmar lives, without knowledge of the fact that Mr. Stepien has criminal record.
24. I have been told that Mr. Cardona's and Mr. Stepien's employment by the private security service has been terminated in light of these issues. To be absolutely clear, I had no prior knowledge of Mr. Stepien's criminal history. Indeed, I was furious when I found out, because I never would have authorized having a convicted criminal perform any

security services or surveillance on my behalf no matter what precautions might have been in place to ensure he acted appropriately.

25. Second, Mr. Parmar submitted two photographs with his affidavit that he says shows automobiles belonging to Mr. Cardona and Mr. Stepien on private property. The first photograph, attached as Exhibit "A", shows a car on what appears to be the front part of a driveway adjacent to a gate that prevents access to the rest of the driveway and the private residence that is some ways behind the gate. The car in the photograph is pointed away from the gate and towards the street, not towards the residence. The second photograph, attached as Exhibit "B", shows an automobile on pavement in an open space with trucks, a shed, construction vehicles, and various other structures in the background. Mr. Parmar says this picture shows a horse farm, and has submitted a form from the Marlboro Township Police Department describing a September 11, 2018 incident when a car registered to Mr. Stepien apparently entered the property of "Baymar Farms."
26. I cannot say whether the incident described in this form, or either or both of these pictures submitted by Mr. Parmar, reflect some form of trespass or other wrongful conduct by Mr. Cardona or Mr. Stepien. To the extent there was such misconduct in the course of their surveillance activities I certainly did not authorize it, desire it, know about it, or approve of it.

Dated: October 24, 2018
Atlanta, Georgia



Chinh Chu

Exhibit B

WIKIPEDIA

Tony Schiena

Tony Schiena a former South African spy turned government defense contractor and actor. He is currently the CEO of MOSAIC (www.mosaicsec.com), that operates in hostile environments. Tony Schiena was featured in the Vice documentary *Superpower for Hire*. He has been credited for exposing ISIS use of chemical warfare against the Kurds in Iraq. Schiena has been a sought-after expert voice by CNN, FOX News, CBC, BBC, ABC and various other networks on the subject of terrorism and espionage, ISIS as well as modern-day slavery.

Tony Schiena	
Born	Antonio Schiena Springs  South Africa
Occupation	Actor
Years active	2004

Biography

A man of diverse experience and accomplishment, having been operational in various capacities on four different continents. A former veteran of the African intelligence and paramilitary community, he operated during a pivotal part of South Africa's history, in which it averted an imminent civil war, abolishment of apartheid and smooth transition of government. Tony has since served in various capacities in the private security sector as well as aiding government and various law enforcement agencies. A Deputy Sheriff in Virginia and a Lieutenant on the ICAC (Internet Crimes Against Children) federal task force and appointed as Special Detective on specific drug interdiction task forces. Tony has numerous other prestigious affiliations and memberships including being a long-standing member of the International Police Association as well as being awarded the rank of Lieutenant Colonel by the Hungarian National Guard for meritorious service.

Tony has been embedded with law enforcement in various capacities for a substantial period of time. He has given specialist instruction to the New York Police Department, South African Police Force, Indianapolis Police Department, Merced County Sheriff Department and SWAT team (during which he operated as team leader of a National Sheriff Associations special operations team for the program "The Sheriff") as well as various military and government agencies including NATO and ISAF (International Security Assistance Force) in Iraq and Afghanistan as well as special operations groups in Kabul and northern Afghanistan, Cambodian special forces, Afghan National Army CID (in Mazar e Sharif Afghanistan), Hungarian and Latvian intelligence and military, Mongolian Quick Reaction Force stationed in Kabul, Croatia special forces, Italian air force etc.

As a sportsman he achieved the highest of accolades, retiring as an undefeated World Heavyweight Karate Champion. Tony has consistently built and improved on his defensive tactics arsenal, becoming one of the premier experts and advisors in the world today.

Tony runs the majority of his current security operations out of his US based company MOSAIC (Multi Operational Security Agency Intelligence Company). Tony has various other strategic security partnerships in New York City and Nevada with former special forces operators, intelligence operators and intelligence heads. His security partnerships extend outside of the US to the cities of London and Dubai and is constantly expanding into other geographical areas and sectors of security.

Tony's endeavors in Iraq and his support of the Kurdish Peshmerga in their struggle as the only organized force against ISIS made worldwide headlines during his exposure of chemical weapon usage by ISIS against the Kurds. Tony trained Kurdish special forces commanders in escape & evasion, defensive tactics and counter insurgency as well as providing

emergency lectures on how to secure front line bases against chemical attacks.

Tony also dedicates time to fighting sex trafficking of children through The Mosaic Federation based in London, UK, in which he shares trusteeship with the current head of Intelligence for Scotland Yard, Commander Richard Martin. Tony has spoken at the United Nations, G20 women's conference in Paris France, the Vatican and various other prestigious platforms on human trafficking. His organization also collaborated with CNN International on a successful, global, strategic communication initiative on modern-day slavery called the HEARD expose.^{[1][2][3][4][5][6][7]}

References

1. <http://www.tonyschiena.com/bio/>
2. "Exclusive photos appear to show grisly effect of ISIS' mustard gas attacks on Kurds" (<http://www.foxnews.com/world/2015/09/09/exclusive-photos-appear-to-show-grisly-effect-isis-mustard-gas-attacks-on-kurds.html>). Fox News. Retrieved 2016-02-09.
3. "CBC National News Top Story" (<http://mosaicsec.com/cbc-national-news-top-story/>). *Mosaicsec.com*. 2015-10-10. Retrieved 2016-02-09.
4. "FOX News – American News hour" (<http://mosaicsec.com/fox-news-american-newshour/>). *Mosaicsec.com*. 2015-02-26. Retrieved 2016-02-09.
5. "Tough men for hire: Ex-special forces in demand for war on terror" (<http://www.foxnews.com/world/2015/02/25/hard-men-for-hire-ex-special-forces-in-demand-for-war-on-terror.html>). Fox News. 2015-02-25. Retrieved 2016-02-09.
6. "7 Life Hacks from a Real-Life Spy | Man's Life" (<http://manslife.com/5666/spy-life-hacks/>). *Manslife.com*. 2015-07-08. Retrieved 2016-02-09.
7. "Superpower for Hire | VICE | United States" (<https://www.vice.com/video/superpower-for-hire-811>). *Vice.com*. Retrieved 2016-02-09.

External links

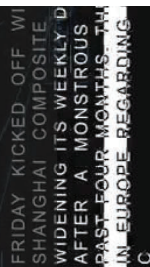
- Tony Schiena (<https://www.imdb.com/name/nm1460101/>) on IMDb

Retrieved from "https://en.wikipedia.org/w/index.php?title=Tony_Schiena&oldid=848835056"

This page was last edited on 4 July 2018, at 17:28 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Exhibit C



EMPOWERING GROWTH SECURELY WITH MOSAIC

To view this content, click [reload](#).

MEET MOSAIC

OUR STORY

MOSAIC was first conceived post 911. The world changed on that day and we would inevitably have to deal with terrorism for the remainder of our lifetimes. As our Chairman stood on the podium as key-note speaker on Narco Terrorism at the NSA Sheriff Annual Convention, he ended his talk by playing an announcement by Baghdad of the formation of a shadowy terrorist organization called ISIS. MOSAIC had been present in Iraq and Afghanistan in various capacities and incarnations for many years and our chairman conducted escape & evasion and defensive tactics instruction on various NATO basis including, under special request, training a newly formed unit of the Afghan National Army. Prior to the Middle Eastern wars, MOSAIC was present in various other conflicts including the border skirmish's between the Thai's and Cambodians. Standing on the NSA podium our Chairman successfully predicated one of the greatest terrorism threats we have faced, ISIS and so MOSAIC deployed to Northern Iraq in the aid of the then, only organized force standing against ISIS, the Kurds.

OUR VISION

MOSAIC, supporting the Kurds in Iraq and working with a NATO country, exposed ISIS use of chemical weapons, conducted emergency lectures on reinforcing frontline bases from chemical and radioactive material and trained Kurdish Special Forces Commanders in counter insurgency, escape & evasion and defensive tactics. Having made a significant impact in the war against ISIS,

MOSAIC transitioned and focused its expertise on the civilian market, partnering with intelligence heads and senior intelligence operatives as well as former special forces group members, it based operations out of London and the US, including partnering with the NSA Sheriff in a training headquarters in Rhode Island called the Global Center for Public Safety. MOSAIC became a rapid response intelligence outfit.

OUR EXPERTISE

MOSAIC, Empowering Growth Securely. A strategic intelligence and advisory firm dedicated to helping clients mitigate exposure and minimize loss, both financially and physically. We integrate technology with specialist knowledge, including human and deep source intelligence, combined with open source, cyber and surveillance intelligence in order to address current and emerging threats to multinational corporations, governments, and non-governmental organizations as well as private individuals, across four main areas: intelligence, counter-terrorism, cyber security, and critical infrastructure protection. MOSAIC management consists of a legal team comprising criminal, civil and human rights attorneys working in tandem with former senior intelligence and special forces members together with former presidential level office public relations experts in both the UK and US in order to ensure strategic communication. We develop long-term relationships with clients as trusted advisors, providing strategic service delivery that is threat driven and intelligence-led.

OUR INTELLIGENCE SERVICES

// ASSET RECOVERY

Why "throw good money after bad?" Criminal groups use elaborate schemes to hide assets from victims, forcing them to write off losses. Assets have been misappropriated, stolen or hidden. MOSAIC's own legal, intelligence and forensic accounting departments work closely with INTERPOL / law enforcement and government officials to lawfully freeze and secure the funds.

Using instruments available through the courts, companies and creditors, victims of fraud can recover the assets they once believed they would never see again.

// CRISIS MANAGEMENT

MOSAIC stands alone in the intelligence sector as a full service security entity that's operated in a boutique fashion. MOSAIC has successfully serviced some of the planet's most influential and powerful people, corporations and governments with the utmost discretion. We have meticulously and successfully handled counter kidnapping operations, extortion and bribery, malicious defrauding, asset tracing and recovery, cyber defense, counter terrorism and human trafficking operations.

// DUE DILIGENCE

When exploring potential alliances, partners, mergers and other investment opportunities, corporations and other business entities need to identify a wide range of variables including personnel issues, fiscal irregularities and true track records. MOSAIC conducts field investigations, interviews, and/or lawful social engineering methods are employed to enhance, further probe or corroborate investigative findings.

OUR SECURITY SERVICES

// CYBER SECURITY

Awarded "Most trusted Cyber Security Firm 2017" GDS review

As leaders in the field of high-level intelligence and physical security infrastructure that offer red team testing, our operators understand security is more than firewalls and software. Our team will perform a full risk assessment of your technological and human factors, utilizing a series of techniques including attacking software and computer systems from the start by scanning ports, and examining known defects and patch installations. Attack types include social engineering, open source research, and deception to attempt a cyber attack in order to bypass and breach your perimeter and physical security, within an agreed set of boundaries.

// EXECUTIVE PROTECTION

MOSAIC has a track record of securing high-value targets including dignitaries under terrorist threat, individuals under threat of government assassination, persons placed in witness protection programs, intelligence operatives operating in hostile environments as well as former Prime Ministers and a President. MOSAIC is now entrusted with the lives of long-standing high net-worth clients, senior executives, families and private individuals who travel frequently overseas and require complete protection solutions that includes travel management, logistical planning, crisis management and emergency coordination, ensuring the safety of people and businesses that may be at risk or exposed due to the nature of their business, status, net worth, association, country of origin or location they are visiting.

MOSAIC is an official partner in SHY AVIATION's Hong Kong office and preferred security vendor of its global operations.

// COUNTER-TERRORISM

MOSAIC has been active in counter terrorism through directives from governments in various capacities. With regards to training provided at the Global Center for Public Safety and other temporary foreign locations.

H.E.A.T. Hostile Environment Advanced Training

Defensive Tactics //

"Not Taken"

We provide a conflict area defensive tactics system incorporating elements of SERE (Survive, Evade, Resist, Escape). This is the most effective Special Forces system taught exclusively to government, military and select law enforcement agencies and SWAT teams. Individuals or groups outside of our usual clientele are highly vetted and screened before selection.

See [GDS Page](#) for Counter Terrorism Training Program

VICE

Superpower for Hire: Rise of the Private Military

► Play Video

i

// Hit Play //

DISCOVER MORE PRESS

GET IN TOUCH

CONTACT US

US Office, Washington DC
+1 202 480 2920

UK Office, London
+44 20 3868 8739

office@mosaicsec.com

VISIT US

Monday - Friday 11:00 - 18:30
Saturday 11:00 - 17:00
Sunday 12:30 - 16:30

SOCIAL

in f G+

TELL US

Name *

Email *

Subject

Message

Send

MosaicSec

10/29/2018

UN Vendor Number: 508777

// Powered by Covert Bear 2018 //

0011478